RECEIVED
CENTRAL FAX CENTER
AUG 2 8 2006

PATENT
Atty Docket No.: 10018744-1

In The U.S. Patent and Trademark Office

Inventor(s):	Zhichen Xu et al.	**Confirmation No.:**	6233
Serial No.:	10/084,436	**Examiner:**	Samson B. Lemma
Filed:	February 28, 2002	**Group Art Unit:**	2132
Title:	INCREASING PEER PRIVACY		

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATE OF FACSIMILE TO THE USPTO

I hereby certify that this correspondence is being transmitted to the Patent and Trademark Office facsimile number (571) 273-8300 on August 28, 2006. This correspondence contains the following document(s):

1 sheet of Transmittal Letter for Appeal Brief (2 copies).

32 sheets of Appeal Brief including Appendices.

Respectfully submitted,

MANNAVA & KANG, P.C.

August 28, 2006

Timothy Kang Reg. No. 46,423

Ashok K. Mannava
Reg. No.: 45,301

MANNAVA & KANG, P.C.
8221 Old Courthouse Road
Suite 104
Vienna, VA 22182
(703) 652-3822
(703) 865-5150 (facsimile)

Intellectual Property Administration
P. O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 10018744-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	Zhichen Xu et al.	**Confirmation No.:**	6233
Application No.:	10/084,436	**Examiner:**	Samson B. Lemma
Filing Date:	Feb. 22, 2002	**Group Art Unit:**	2132
Title:	INCREASING PEER PRIVACY		

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Sir:

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on June 1, 2006.

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) $500.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

( ) (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d) for the total number of months checked below:

( )	one month	$120.00
( )	two months	$450.00
( )	three months	$1020.00
( )	four months	$1590.00

( ) The extension fee has already been filled in this application.

(X) (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of $500.00. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees. A duplicate copy of this sheet is enclosed.

( ) I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, Alexandria, VA 22313-1450. Date of Deposit:_____

OR

(X) I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number (571) 273-8300 on Aug. 28, 2006

Number of pages: 35

Typed Name: Judy H. Chung

Respectfully submitted,

Zhichen Xu et al.

By /Timothy Kang/ Reg. No. 46,423

Ashok K. Mannava

Attorney/Agent for Applicant(s)
Reg. No. 45,301

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

Attorney Docket No.: 10018744-1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	Zhichen Xu et al.	**Confirmation No.:**	6233
Serial No.:	10/084,436	**Examiner:**	Samson B. Lemma
Filed:	February 28, 2002	**Group Art Unit:**	2132
Title:	INCREASING PEER PRIVACY		

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF - PATENTS

Sir:

This is an Appeal Brief in connection with the decisions of the Examiner in an Office Action dated April 10, 2006 and a Notice of Panel Decision from Pre-Appeal Brief Review dated August 1, 2006. It is respectfully submitted that the present application has been more than twice rejected. Each of the topics required in an Appeal Brief and a Table of Contents are presented herewith and labeled appropriately.

08/29/2006 EAREGAY1 00000068 082025 10084436
01 FC:1402 500.00 DA

RECEIVED
CENTRAL FAX CENTER
AUG 2 8 2006

PATENT

Atty Docket No.: 10018744-1
App. Ser. No.: 10/084,436

TABLE OF CONTENTS

PATENT

Atty Docket No.: 10018744-1
App. Ser. No.: 10/084,436

(1) **Real Party In Interest**

The real party in interest is Hewlett-Packard Development Company, L.P.

(2) **Related Appeals and Interferences**

There are no other appeals or interferences related to this case.

(3) **Status of Claims**

Claims 1-36 are pending and rejected. All pending claims are hereby appealed.

(4) **Status of Amendments**

No amendments were filed subsequent to the Final Rejection in the Office Action mailed April 10, 2006.

(5) **Summary of Claimed Subject Matter**

A conventional system of network nodes (or peers) interconnected via a network provides a relatively convenient means of exchanging information between the peers. However, the conventional network system may be vulnerable to malicious users. For example, by monitoring the network traffic on the network, malicious users may determine the types of information stored at specific peers. This may be problematic if one of the peers is a source of sensitive information.

According to an embodiment described in the Applicant's specification, peers to be used in a network path are predetermined, and a mix anonymously identifying the peers in the path is created and used to transmit a reference to the requested data, such as a URL, along

the path from a data provider peer having the requested information to a data requestor peer requesting the information. For example, a data requestor peer sends a request for data to a trusted third party peer. The trusted third party peer searches a directory to identify a peer storing the requested information. If a peer is storing the requested information, the trusted third party peer selects multiple peers to be used in a path between the data provider peer and the data requestor peer. The selected peers include multiple peers between the data requestor peer and the data provider peer in the path. The trusted third party peer builds a mix anonymously identifying the peers in the path, and sends the mix to the data provider peer. The data provider peer uses the mix to identify the next peer in the path to the data requestor peer, and sends the mix and a reference to the requested data to the next peer in the path. See page 9, lines 1-17; page 17, line12-page 20, line 22; see figures 4A-B.

Intermediate peers in the predetermined path receive the mix, update the mix, and use the mix to forward the reference to the requested information to the next peer in the path until the reference to the requested information reaches the data requestor. See page 9, line 18-page 10, line 22; page 21 line 1-page 22, line 11; see figure 5.

Also, the mix may include a decoy or fake mix and the fake mix is used to keep the identity of the data requestor anonymous from a last peer in the mix before the data requestor. See page 19, lines 15-22.

Accordingly, by utilizing the embodiments, the identity of a data requestor and a data provider are afforded a level of protection during a data transfer. Moreover, the trusted third party peer may avoid becoming a throughput bottleneck for the overall system because the trusted third party directs data to be transferred between parties. See page 10, lines 18-22.

Support in the specification for independent claims 1, 14, 18, 22 and 24 is as follows:

1. A method of increasing peer privacy in a computer network including peers operable to exchange information via the network, wherein the peers include computing platforms, the method comprising (See page 9, lines 1-17; page 17, line12-page 20, line 22; see figures 4A-B):

receiving a request for data from a data requestor (See page 17, lines 18-22);

determining whether a data provider exists that stores the requested data; wherein the data provider is a peer of the peers (See page 18, lines 1-16);

selecting a plurality of the peers to form a path between said data provider and said data requestor, wherein said data provider and said data requestor are the respective ends of said path (See page 18, lines 11-20);

generating a mix according to said path, wherein the mix includes an anonymous identity of each of the plurality of peers in the path (See page 18, lines 21-page 20, line 18); and

transmitting said mix to said data provider (See page 20, lines 19-22).

14. A method of increasing peer privacy in a computer network including peers operable to exchange information via the network, wherein the peers include computing platforms, the method comprising (See page 9, line 18-page 10, line 22; page 21 line 1-page 22, line 11; see figure 5):

receiving a message comprising a mix at a current peer, wherein the mix includes an anonymous identity of each of a plurality of peers in a path between a data provider and a data requestor in the network (See page 21, lines 7-12);

modifying said mix by applying a complementary encryption key of said current peer to said mix (See page 21, line 13-page 22, line 8);

retrieving a subsequent peer to said current peer (See page 21, line 13-page 22, line 8);

modifying said message with said modified mix (See page 21, line 13-page 22, line 8); and

transmitting said modified message to said subsequent peer (See page 22, lines 9-11).

18. A system for increasing privacy in a computer network including peers operable to exchange information via the network, wherein the peers include computing platforms, the system comprising(See figures 1, 3 and 7; see page 15, line 3-page 17, line 11; page 9, lines 1-17; page 17, line12-page 20, line 22; see figures 4A-B):

at least one processor (See page 23, line 21-page 24, line 16; see figures 3 and 7; see page 15, line 3-page 17, line 11);

memory coupled to said at least one processor (See page 23, line 21-page 24, line 16; see figures 3 and 7; see page 15, line 3-page 17, line 11); and

a privacy module residing in said memory and said privacy module executed by said at least one processor, wherein said privacy module is configured to (See page 23, line 21-page 24, line 16; see figures 3 and 7; see page 15, line 3-page 17, line 11):

receive a request for a data from a data requestor (See page 17, lines 18-22);

determine whether a data provider exists that stores the requested data; wherein the data provider is a peer of the peers (See page 18, lines 1-16);

select a plurality of the peers to form a path between said data provider and said data requestor, wherein said data provider and said data requestor are the respective ends of said path (See page 18, lines 11-20);

generate a mix according to said path, wherein the mix includes an anonymous identity of each of the plurality of peers in the path (See page 18, lines 21-page 20, line 18); and

transmit said mix to said data provider (See page 22, lines 9-11).

22. An apparatus for increasing privacy in a computer network including peers operable to exchange information via the network, wherein the peers include computing platforms, the apparatus comprising (See figures 1, 2 and 7; see page 11, line 1-page 14, line 18; See page 9, line 18-page 10, line 22; page 21 line 1-page 22, line 11; see figure 5):

at least one processor (See page 23, line 21-page 24, line 16; see figures 2 and 7);

memory coupled to said at least one processor (See page 23, line 21-page 24, line 16; see figures 2 and 7); and

a privacy module residing in said memory and said privacy module executed by said at least one processor, wherein said privacy module is configured to receive a message at said data provider, said message comprises (See page 21, lines 10-12; page 11, line 1-page 14, line 18; see figures 2 and 7):

a mix configured to provide a path among a plurality of the peers between a data provider and a data requestor in the network, wherein the mix includes an anonymous identity of each of the plurality of peers in the path (See page 19, lines 11-22);

an encrypted reference to requested data encrypted with a first encryption key (See page 19, lines 11-22; page 21, lines 18-22);

an encrypted first encryption key protected with a public key of said data requestor (See page 19, lines 11-22; page 21, lines 13-17); and

said privacy module is also configured to decrypt said first encryption key with a complementary encryption key to said public key of said data provider and to decrypt said data reference with said first encryption key (See page 19, lines 11-22; page 21, lines 13-17).

24. A computer readable storage medium on which is embedded one or more computer programs, said one or more computer programs implementing a method of increasing peer privacy in a computer network including peers operable to exchange information via the network, wherein the peers include computing platforms, said one or more computer programs comprising a set of instructions for (See figures 3 and 7; see page 23, line 21-page 25, line 9):

receiving a request for data from a data requestor (See page 17, lines 18-22);

determining whether a data provider exists that stores the requested data; wherein the data provider is a peer of the peers (See page 18, lines 1-16);

selecting a plurality of the peers to form a path between said data provider and said data requestor, wherein said data provider and said data requestor are the respective ends of said path (See page 18, lines 11-20);

generating a mix according to said path, wherein the mix includes an anonymous identity of each of the plurality of peers in the path (See page 18, lines 21-page 20, line 18); and

transmitting said mix to said data provider (See page 20, lines 19-22).

(6) Grounds of Rejection to be Reviewed on Appeal

Whether claims 1-36 are unpatentable over Walker et al. (5,862,223), referred to as Walker, in view of Herz (6,460,036).

Claim 4 was objected to in the final rejection mailed 4/10/06 because it depends on itself. This objection is not being appealed. As correctly noted in the objection, claim 4 was intended to be dependent on claim 3, and claim 4 will be amended accordingly if prosecution is re-opened.

(7) Arguments

The test for determining if a claim is rendered obvious by one or more references for purposes of a rejection under 35 U.S.C. § 103 is set forth in MPEP § 706.02(j):

> To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed

> combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

Therefore, if the above-identified criteria are not met, then the sited reference(s) fails to render obvious the claimed invention and, thus, the claimed invention is distinguishable over the sited reference(s).

According to embodiments described in the Applicants' specification, an anonymous network path is determined and formed between peers in a computer network, wherein the peers include computing platforms. Multiple peers between the data requestor and the data provider are included in the path. Peers may exchange data using the anonymous network path, and the anonymous network path minimizes the ability of malicious users determining the source or destination of sensitive information.

Walker is completely unrelated to forming anonymous network paths. Walker, in contrast, describes a method for an end user to get answers from experts. For example, an end user needs expert review of an academic paper or needs an answer to a question about running the user's business. See column 11, lines 12-55. The end user submits a request for a human expert qualified to respond to the user's question to a controller. Walker refers to the controller as a human, such as Carol. See columns 35-36. The controller searches a database for an expert that is qualified to respond to the user request. The controller sends the request to an expert if a qualified expert is found. The expert sends an answer to the controller and the controller sends the answer to the user. See columns 35-36.

Arguments With Respect to Claim 1

Walker in view of Herz fails to teach or suggest many of the features of independent claim 1.

- Claim 1 recites peers include computing platforms and "determining whether a data provider exists that stores the requested data, wherein the data provider is a peer of the peers."

The rejection of claim 1 alleges that determining whether a computing platform exists that stores requested data is taught by Walker. Specifically, the rejection states,

> As explained on column 35, line 32b, Bob's computer is also qualified expert. Bob's computer is acts as both client and server when interacts with carol's computer and is assumed to be a modern PC which meets the limitation of a peer and since there are a number of experts, the qualified expert who would be selected to provide the an expert answer, or Bob's computer meets the limitation of peer of peers and carol's computer or the central controller determines whether a data provider for instance Bob's computer exists that stores the requested data)

A controller, such as a person (*i.e.*, Carol), in Walker receives an expert request/requested data and a search program identifies an expert, such as Bob, qualified to respond to the experts. Walker discloses selecting an expert qualified to respond to a request. However, Walker fails to teach or suggest determining whether a computer stores the requested data. Selecting a qualified expert is not the same as determining whether a computer exists that stores the requested data. Claim 1 does not recite selecting a qualified expert or selecting a qualified expert's computer. Instead, claim 1 recites determining whether a data provider (*i.e.*, computing platform) exists that stores the requested data.

Walker only discloses selecting an expert that is allegedly qualified to respond to a request, but does not determine whether the expert stores requested data in a computer or otherwise knows the answer to a request. Simply because an expert in Walker may store an answer in his/her computer after determining the answer does not require making a determination of whether an expert's computer exists which stores the answer.

The rejection of claim 1, referring to the feature of determining whether a data provider exists that stores the requested data, also alleges that this is taught by the procedure in Walker that uses a peer review to determine whether an expert is qualified to respond to a request. As described above, determining whether an expert is qualified to respond to a request is not the same as determining whether a computer stores requested data.

The rejection of claim 1 further alleges Herz discloses determining whether a data provider exists that stores requested data in column 38, lines 31-47 (S4). Herz discloses that after a user has registered with the proxy server S2, the user may use the services of the proxy server to interact with service providers. For example, the user sends a request to S2 to communicate with the server S4 using a pseudonym P. However, Herz fails to teach or suggest determining whether the server S4 or any other server stores requested data. Instead, Herz simply transmits a message to a destination using a pseudonym P. Unlike the trusted third party peer in an embodiment of the Applicant's specification, which may use a directory 320 of information stored at each peer for determining whether a peer stores the requested data, there is no determination made in Herz or Walker.

- Claim 1 recites, "selecting a plurality of the peers to form a path between said data provider and said data requestor, wherein said data provider and said data requestor are the respective ends of said path."

The rejection of claim 1 alleges Walker teaches this feature and specifically refers to columns 8, 35 and 36 of Walker to teach this feature and also states "experts/data providers/peers can be chosen or selected as disclosed on column 8, lines 52-53; therefore if the experts answers comes from a plurality of experts for the same data request, the controller will inherently form a path between said provider and data requestor."

Walker fails to teach or suggest selecting a plurality of peers between a data provider and a data requestor. Columns 35-36 of Walker describe an example of submitting and responding to an end user request. Alice the end user submits a request to the trusted third party/central controller, Carol. Carol selects an expert, Bob, for responding to the request. Carol sends the request to Bob. Bob sends the answer to Carol and Carol sends the answer to Alice. The path in Walker only includes a single person, Carol, between the data provider, Bob, and the data requestor, Alice. Thus, Walker fails to teach or suggest selecting a plurality of peers between a data provider and a data requestor.

The rejection alleges that selecting a plurality of the peers is inherent in Walker because if the experts' answers come from a plurality of experts for the same data request, the controller will inherently form a path between said provider and data requestor.

On the contrary, the controller may simply forward the answers from each expert to the requestor. However, the controller does not select a plurality of peers to be used between the data provider and the data requestor for transmitting the requested data to the data requestor. In claim 1, the plurality of peers to be used in a path between the data provider and the data requestor are pre-selected, and then included in a mix which is transmitted to the data provider. The controller in Walker does not pre-select a plurality of peers between the data provider and the data requestor for use in the path.

Furthermore, it is not inherent in Walker that the controller of Walker forms a path between said provider and data requestor. A claim element not explicitly taught by the prior art may be an inherent feature of the prior art. However, it is the burden of the Examiner and not the Applicants to prove that the claimed feature is inherent. Secondly, to establish inherency, the Examiner must make clear that the missing descriptive matter is *necessarily present* in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. "Inherency, however, *may not be established by probabilities or possibilities*. The mere fact that a certain thing may result from a given set of circumstances is not sufficient." *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999) (citations omitted).

As described above, the controller in Walker, which is Carol, only selects an expert and sends the request to the expert. No path is formed by the controller and no selection of a plurality of peers between the data provider and requestor is performed by the controller. Sending a request to an expert does not require the controller to form a path. The data sent to the requestor may follow a network path when transmitted to the requestor, but the path is not necessarily predetermined. Instead, the routing protocol may determine the path as the data is being routed to the requestor.

Also, in Walker, if a plurality of experts is responding to a single request, Walker fails to teach or suggest that each expert selects a plurality of peers to be used in path. Columns 35 and 36 of Walker cited in the rejection fail to teach or suggest a plurality of peers are selected by Carol or Bob to be used in the path between Bob and Alice. Herz also fails to teach or suggest selecting a plurality of the peers between said data provider and said data requestor to form a path between said data provider and said data requestor.

- Claim 1 also recites, "generating a mix according to said path, wherein the mix includes an anonymous identity of each of the plurality of peers in the path; and transmitting said mix to said data provider."

The office action including the final rejection correctly states on page 4 that Walker does not disclose a mix configured to provide a path. However, the rejection alleges Herz discloses the mix in column 39 as a "set of mixes".

Mixes are described in Herz as an anonymizing mix protocol as taught by D.Chaum in the paper titled "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communications of the ACM, Volume 24, Number 2, February 1981. This mix procedure provides untraceable secure anonymous mail between two parties with blind return addresses through a set of forwarding and return mounting servers termed "mixes". See column 34, line 61-column 35, line 40.

Herz, however, fails to teach or suggest that the mix protocol includes selecting all the servers or peers in the path before transmitting the mail through a set of forwarding and return mounting servers termed "mixes". Instead, the mix protocol may anonymously select servers or peers in the path as the data is transmitted. Claim 1 recites selecting the peers to form the path and generating the mix from the selected peers, and then transmitting the mix to the data provider. Thus, the peers for the path are pre-selected and the mix is generated from the pre-selected peers and then the entire mix is transmitted to the data provider so the data provider can use the mix to send the requested data to the data requestor. The mix procedure of Herz does not disclose pre-selecting the peers to be used in the mix.

- Furthermore, the mix is not transmitted to the data provider, which is the server S4 in Herz as previously alleged in the rejection of claim 1 on page 8 of the office

action. The server S4 does not receive the mix. Instead; the mix is only sent to the proxy server 82, which is a proxy server and not a data provider. See column 39, line 6-column 40, line 6 of Herz. Accordingly, Herz fails to teach or suggest transmitting said mix to said data provider. Walker also fails to teach or suggest transmitting a mix including a plurality of pre-selected peers to the data provider.

- Furthermore, the rejection of claim 1 fails to establish a *prima facie* case of obviousness because no motivation was provided for combining the alleged teaching of determining whether a data provider exists that stores requested data in column 38 of Herz with Walker. The rejection of claim 1 states on page 8 of the office action that Herz discloses determining whether a data provider exists storing the requested data. However, the motivation states that it would have been obvious "to combine the features of generating a mix according to the path wherein the mix includes an anonymous identity of each of the plurality of peers in the path as per teachings of Herz to the method as taught by Walker, in order to provide a secure communication and protection against eavesdropper." This motivation does not apply for combining the alleged "determining whether a data provider exists storing the requested data" of Herz with Walker.

For at least these reasons, it is respectfully submitted that the Examiner failed to establish a *prima facie* case of obviousness against claims 1-13. Consequently, it is respectfully submitted that these claims are allowable over the prior art of record.

Arguments with respect to independent claims 18 and 24

Independent claim 18 recites the peers include computer platforms and the following:

determine whether a data provider exists that stores the requested data; wherein the data provider is a peer of the peers;

select a plurality of the peers to form a path between said data provider and said data requestor, wherein said data provider and said data requestor are the respective ends of said path;

generate a mix according to said path, wherein the mix includes an anonymous identity of each of the plurality of peers in the path; and

transmit said mix to said data provider.

Independent claim 24 recites similar features. These features are not taught or suggested by Walker in view of Herz for the reasons stated above with respect to claim 1. Accordingly, it is respectfully submitted that the Examiner failed to establish a *prima facie* case of obviousness against claims 18-21 and 24-36. Consequently, it is respectfully submitted that these claims are allowable over the prior art of record.

Arguments with respect to independent claims 14 and 22

Independent claim 14 recites receiving a mix wherein the mix includes an anonymous identity of each of a plurality of peers in a path between a data provider and a data requestor in the network. Thus, the mix includes a plurality of pre-selected peers between the data provider and the data requestor. Walker in view of Herz fails to teach or suggest a mix including a plurality of pre-selected peers between the data provider and the data requestor for the reasons stated above with respect to claim 1.

Also, the rejection of claim 14 alleges Walker discloses the mix including an anonymous identity of each of the plurality of peers. Walker discloses messages are made anonymous by varying the length and timing of delivery. See column 34, lines 5-6.

However, Walker fails to teach anonymous identifiers for each of a plurality of peers in the path. Herz also fails to teach or suggest an anonymous identity of each of the plurality of peers in the path between the data provider and the data requestor. Herz discloses using a proxy server to keep the data requestor anonymous but does not disclose an anonymous identity of each of the plurality of peers in the path between the data provider and the data requestor.

Independent claim 22 recites features similar to the features described above with respect to independent claim 14. Accordingly, it is respectfully submitted that the Examiner failed to establish a *prima facie* case of obviousness against claims 14-17 and 22-23. Consequently, it is respectfully submitted that these claims are allowable over the prior art of record.

Arguments with respect to dependent claims 8, 9, 17, 31 and 32.

Dependent claims 8, 9, 17, 31 and 32 are believed to be allowable for at least the reasons their respective independent claims are believed to be allowable. Furthermore, these claims recite a decoy mix.

According to an embodiment described in the Applicant's specification, the mix may include a decoy or fake mix, and the fake mix is used to keep the identity of the data requestor anonymous from a last peer in the mix before the data requestor. See page 19, lines 15-22.

The claimed decoy mix is not mentioned in the rejection of these claims. Also, the claimed decoy mix is not taught or suggested by Walker in view of Herz.

PATENT

Atty Docket No.: 10018744-1
App. Ser. No.: 10/084,436

(8) Conclusion

For at least the reasons given above, the rejections of claims 1-36 are improper. Accordingly, it is respectfully requested that such rejections by the Examiner be reversed and these claims be allowed. Attached below for the Board's convenience is an Appendix of claims 1-36 as currently pending.

Please grant any required extensions of time and charge any fees due in connection with this Appeal Brief to deposit account no. 08-2025.

Respectfully submitted,

Dated: August 28, 2006 By Timothy Kang Reg. No. 46,423
Ashok K. Mannava
Registration No.: 45,301

MANNAVA & KANG, P.C.
8221 Old Courthouse Road
Suite 104
Vienna, VA 22182
(703) 652-3822
(703) 865-5150 (facsimile)

(9) Claim Appendix

1. A method of increasing peer privacy in a computer network including peers operable to exchange information via the network, wherein the peers include computing platforms, the method comprising:

receiving a request for data from a data requestor;

determining whether a data provider exists that stores the requested data; wherein the data provider is a peer of the peers;

selecting a plurality of the peers to form a path between said data provider and said data requestor, wherein said data provider and said data requestor are the respective ends of said path;

generating a mix according to said path, wherein the mix includes an anonymous identity of each of the plurality of peers in the path; and

transmitting said mix to said data provider.

2. The method according to claim 1, further comprising:

generating a first encryption key; and

encrypting said first encryption key with a public encryption key of said data provider.

3. The method according to claim 2, further comprising:

encrypting said reference to said data with said first encryption key; and

encrypting said first encryption key with a public encryption key of said data requestor.

4. The method according to claim 4, further comprising:

transmitting said encrypted first encryption key with said public key of said data provider, said encrypted reference to said data, said mix, said first encryption key with said public encryption key of said data requestor to said data provider as a message to said data provider.

5. The method according to claim 4, further comprising:

receiving said message at said data provider;

decrypting said first encryption key with a complementary encryption key to said public key of said data provider; and

decrypting said data reference with said first encryption key.

6. The method according to claim 5, further comprising:

modifying said mix with said complementary encryption key to obtain a subsequent peer to said data provider along said path;

retrieving said data according to said data reference;

encrypting said data with said first encryption key; and

transmitting said modified mix to said subsequent peer along with encrypted data and said first encryption key with said public encryption key of said data requestor as a modified message.

7. The method according to claim 5, further comprising:

receiving said modified message at a current peer along said path;

modifying said mix with a complementary encryption key of said current peer to obtain a next peer along said path; and

transmitting said modified mix along with said encrypted data and said first encryption key of said data requestor as another modified message to said next peer.

8. The method according to claim 1, wherein said generation of said mix further comprises:

generating a decoy mix.

9. The method according to claim 8, further comprising:

forming a tuple comprising said data requestor and said decoy mix; and

modifying said mix by encrypting said tuple with an encryption key of a peer subsequent to said data provider in said path.

10. The method according to claim 9, wherein said encryption key comprises an public encryption key.

11. The method according to claim 10, wherein said public encryption key is generated by one of an asymmetric encryption algorithm.

12. The method according to claim 1, wherein said generation of said mix further comprises:

selecting a current peer along said path;

forming a current tuple comprising said current peer and a previous mix; and

modifying said mix at said current peer by encrypting said current tuple with an encryption key of a subsequent peer to said current peer in said path.

13. The method according to claim 12, further comprising:

repeating said formation and modification until said current peer being said data provider.

14. A method of increasing peer privacy in a computer network including peers operable to exchange information via the network, wherein the peers include computing platforms, the method comprising:

receiving a message comprising a mix at a current peer, wherein the mix includes an anonymous identity of each of a plurality of peers in a path between a data provider and a data requestor in the network;

modifying said mix by applying a complementary encryption key of said current peer to said mix;

retrieving a subsequent peer to said current peer;

modifying said message with said modified mix; and

transmitting said modified message to said subsequent peer.

15. The method according to claim 14, further comprising:

selecting a plurality of peers to form said path; and

generating said mix according to said path.

16. The method according to claim 14, further comprising:

adding encrypted requested data to said message from the data provider.

17. The method according to claim 14, further comprising:

generating a decoy mix, wherein said mix includes said decoy mix.

18. A system for increasing privacy in a computer network including peers operable to exchange information via the network, wherein the peers include computing platforms, the system comprising:

at least one processor;

memory coupled to said at least one processor; and

a privacy module residing in said memory and said privacy module executed by said at least one processor, wherein said privacy module is configured to:

receive a request for a data from a data requestor,

determine whether a data provider exists that stores the requested data; wherein the data provider is a peer of the peers;

select a plurality of the peers to form a path between said data provider and said data requestor, wherein said data provider and said data requestor are the respective ends of said path;

generate a mix according to said path, wherein the mix includes an anonymous identity of each of the plurality of peers in the path; and

transmit said mix to said data provider.

19. The system according to claim 18, wherein said privacy module is also configured to generate a first encryption key and to encrypt said first encryption key with a public encryption key of said data provider.

20. The system according to claim 19, wherein said privacy module is further configured to encrypt said reference to said data with said first encryption key and to encrypt said first encryption key with a public encryption key of said data requestor.

21. The system according to claim 20, wherein said privacy module is further configured to transmit said encrypted first encryption key with said public key of said data provider, said encrypted reference to said data, said mix, said first encryption key with said public encryption key of said data requestor to said data provider as a message to said data provider.

22. An apparatus for increasing privacy in a computer network including peers operable to exchange information via the network, wherein the peers include computing platforms, the apparatus comprising:

at least one processor;

memory coupled to said at least one processor; and

a privacy module residing in said memory and said privacy module executed by said at least one processor, wherein said privacy module is configured to receive a message at said data provider, said message comprises:

a mix configured to provide a path among a plurality of the peers between a data provider and a data requestor in the network, wherein the mix includes an anonymous identity of each of the plurality of peers in the path;

an encrypted reference to requested data encrypted with a first encryption key;

an encrypted first encryption key protected with a public key of said data requestor; and

said privacy module is also configured to decrypt said first encryption key with a complementary encryption key to said public key of said data provider and to decrypt said data reference with said first encryption key.

23. The system according to claim 22, wherein said privacy module is further configured to:

modify said mix with said complementary encryption key to obtain a subsequent peer to said data provider along said path;

retrieve said data according to said data reference.

encrypt said data with said first encryption key; and

transmit said modified mix to said subsequent peer along with encrypted data and said first encryption key with said public encryption key of said data requestor as a modified message.

24. A computer readable storage medium on which is embedded one or more computer programs, said one or more computer programs implementing a method of

increasing peer privacy in a computer network including peers operable to exchange information via the network, wherein the peers include computing platforms, said one or more computer programs comprising a set of instructions for:

receiving a request for data from a data requestor;

determining whether a data provider exists that stores the requested data; wherein the data provider is a peer of the peers;

selecting a plurality of the peers to form a path between said data provider and said data requestor, wherein said data provider and said data requestor are the respective ends of said path;

generating a mix according to said path, wherein the mix includes an anonymous identity of each of the plurality of peers in the path; and

transmitting said mix to said data provider.

25. The computer readable storage medium in according to claim 24, said one or more computer programs further comprising a set of instructions for:

generating a first encryption key; and

encrypting said first encryption key with a public encryption key of said data provider.

26. The computer readable storage medium in according to claim 25, said one or more computer programs further comprising a set of instructions for:

encrypting said reference to said data with said first encryption key; and

encrypting said first encryption key with a public encryption key of said data requestor.

27. The computer readable storage medium in according to claim 26, said one or more computer programs further comprising a set of instructions for:

transmitting said encrypted first encryption key with said public key of said data provider, said encrypted reference to said data, said mix, said first encryption key with said public encryption key of said data requestor to said data provider as a message to said data provider.

28. The computer readable storage medium in according to claim 27, said one or more computer programs further comprising a set of instructions for:

receiving said message at said data provider;

decrypting said first encryption key with a complementary encryption key to said public key of said data provider; and

decrypting said data reference with said first encryption key.

29. The computer readable storage medium in according to claim 28, said one or more computer programs further comprising a set of instructions for:

modifying said mix with said complementary encryption key to obtain a subsequent peer to said data provider along said path;

retrieving said data according to said data reference;

encrypting said data with said first encryption key; and

transmitting said modified mix to said subsequent peer along with encrypted data and said first encryption key with said public encryption key of said data requestor as a modified message.

30. The computer readable storage medium in according to claim 29, said one or more computer programs further comprising a set of instructions for:

receiving said modified message at a current peer along said path;

modifying said mix with a complementary encryption key of said current peer to obtain a next peer along said path; and

transmitting said modified mix along with said encrypted data and said first encryption key of said data requestor as another modified message to said next peer.

31. The computer readable storage medium in according to claim 24, said one or more computer programs further comprising a set of instructions for:

generating a decoy mix.

32. The computer readable storage medium in according to claim 31, said one or more computer programs further comprising a set of instructions for:

forming a tuple comprising said data requestor and said decoy mix; and

modifying said mix by encrypting said tuple with an encryption key of a peer subsequent to said data requestor in said path.

33. The computer readable storage medium in according to claim 32, said one or more computer programs further, wherein said encryption key comprises an public encryption key.

34. The computer readable storage medium in according to claim 33, said one or more computer programs further, wherein said public encryption key is generated by one of a symmetric encryption algorithm and an asymmetric encryption algorithm.

35. The computer readable storage medium in according to claim 24, said one or more computer programs further, , wherein said generation of said mix further comprises:

selecting a current peer along said path;

forming a current tuple comprising said current peer and a previous mix; and

modifying said mix at said current peer by encrypting said current tuple with an encryption key of a subsequent peer to said current peer in said path.

36. The computer readable storage medium in according to claim 35, said one or more computer programs further comprising a set of instructions for:

repeating said formation and modification until said current peer being said data provider.

(10) Evidence Appendix

None.

PATENT

Atty Docket No.: 10018744-1
App. Ser. No.: 10/084,436

(11) Related Proceedings Appendix

None.